ABSTRACT

A computer-representable object (including, without limitation, a cryptographic key, or a graph or a Boolean description of a system) is secured using a generalized camouflaging technique. The secured object need not be stored in the system, not even in encrypted form. Instead, the technique employs a composition function that regenerates the secured object when one inputs a valid password (which may be any computer-representable information held by a user). By regenerating the secured object each time a valid password is entered, there is no need to store the secured object. If one inputs an invalid password, the technique may generate an incorrect object, such that the user is unable to distinguish this incorrect object from the secured object. If the user tries to use the incorrect object, the user can be exposed as unauthorized, without the user's knowledge that he has been exposed.

52